1 ESCOPO DO SERVIÇO

Todas as atividades previstas e os entregáveis dos serviços de segurança contemplados nessa proposta técnica e comercial para o cliente estarão descritos nesse item.

1.1 INFORMAÇÕES DO AMBIENTE DO CLIENTE

A solução apresentada nessa proposta técnica e comercial foi baseada nas informações e visibilidade do ambiente de T.I. fornecidas cliente.

Caso em qualquer momento do processo de venda, implantação ou operação encontre alguma necessidade adicional decorrente de uma nova informação enviada pelo (a) <NOME DO CLIENTE>, será necessário a avaliação e poderá ter custos adicionais.

1.2 INFRAESTRUTURA TECNOLÓGICA

A VIVO poderá disponibilizar hardware e software compatíveis para a prestação do serviço. Essa infraestrutura é fornecida em regime de comodato, onde os equipamentos são de propriedade da VIVO e fornecidos para o cliente a fim de viabilizar a prestação do serviço.

1.3 ATIVAÇÃO E CONFIGURAÇÃO DO SERVIÇO

A VIVO irá disponibilizar especialista em segurança da informação para conduzir as etapas necessárias para a ativação do serviço ***"in-loco"*** na localidade do (a) <NOME DOCLIENTE>.

Abaixo estão assinaladas com "sim" as atividades que serão realizadas para a ativação do serviço. Caso tenha necessidade de alguma etapa que não foi contemplada na tabela abaixo, deve-se solicitar a inclusão.

		Atividade considerada no escopo?	Detalhamento da execução das atividades
1	Integração da base de usuários (AD)	Sim	Integrar todas as filiais com base de usuários local.
2	Criação de Perfis de acesso com base em usuários	Sim	Criação de políticas de UTM considerando o nível diretor, gerente e coordenador para todas as filiais.
3	Criação de VLANS	Sim	Criar até 3 VLANS para cada localidade.
4	Ativação de Access Points conectados na controladora	Sim	Ativar até 7 (sete) pontos de acesso Wi-fi para cada localidade.
5	Criação e alteração de VPN IPSec.	Não	Não está contemplado a criação de VPN IPSec.
6	Criação e alteração de VPN Site-to-Site	Sim	Criar VPN Site-to-Site entre as filiais Sorocaba e São Paulo.

7	Criação e alteração de VPN Client-to-Site	Sim	Ativar a funcionalidade e criar VPN para a rede de trabalho remoto para a filial SP.
8	Criação e alteração de Balanceamento de link	Sim	Ativar a funcionalidade e criar regras de balanceamento nas filiais São Paulo e Rio de Janeiro.
9	Criação e alteração de Firewall (NGFW)	Sim	Ativar a funcionalidade e configurar as regras de firewall em cada filial de acordo com a política.
10	Criação e alteração de IPS / IDS	Não	O escopo da atividade não contempla ativar a funcionalidade de IPS/IDS.
11	Ativação de H.A. (Passivo)	Não	Não está contemplado H.A. em nenhuma das filiais objeto dessa proposta.

1.4 SERVIÇOS GERENCIADOS: MANUTENÇÃO, SUPERVISÃO E ADMINISTRAÇÃO

1.4.1 Módulo: Manutenção

Este serviço funciona como uma camada de gestão do processo conhecido como RMA (sigla em inglês de *return merchandise authorization*) e fornece ao cliente o suporte técnico e processual para realizar o diagnóstico de eventos de falha nos ativos de segurança escopo dessa proposta técnica e comercial.

1.4.1.1 Como funciona?

Através da análise dos logs gerados pelo equipamento, o SOC juntamente com o fabricante determina se houve alguma avaria em algum dos componentes de hardware e identifica se existe a necessidade de substituição desse equipamento.

Uma vez que o cliente identifica o mau funcionamento de um equipamento de segurança, abre-se um chamado no SOC para avaliação e diagnóstico do problema. O SOC, como parte do processo de análise, solicita ao cliente o envio de determinados logs do equipamento. Com posse de todas as informações, o SOC avalia junto com o fabricante a questão.

Uma vez identificada uma falha de hardware, o SOC inicia o processo de RMA do mesmo, tornando-se a interface do cliente de todo o processo perante o fabricante.

1.4.1.2 Atividades e custos adicionais

Os possíveis custos de logística e emissão de notas fiscais para o envio do componente com avaria não estão inclusos na prestação do serviço, assim como os custos para desinstalação, preparo do equipamento defeituoso e a instalação de um novo equipamento.

1.4.1.3 Atendimento

Na tabela abaixo é possível acompanhar a janela de atendimento para o serviço de Manutenção para cada tipo de atividade.

Serviço	Atendimento a		
	Incidentes	Solicitações	Consultas
Manutenção	24x7	12x7	12x7

Manutenção – Atendimento e Suporte

1.4.1.4 Consultas

São previstas as seguintes consultas para este serviço:

- Lista de equipamentos inclusos no serviço de Manutenção;
- Mapa de rede e de serviços;
- Lista de contatos autorizados pelo cliente.

1.4.1.5 Solicitações

São previstas as seguintes solicitações para este serviço:

- Manutenção em um equipamento individual;
- Manutenção massiva em uma lista de equipamentos;
- Modificação na lista de contatos autorizados do cliente;
- Modificação no mapa de rede ou no mapa de serviços do cliente;
- Modificação de endereço ou contato de acesso a um endereço (o novo endereço será avaliado pelo SOC em relação à área geográfica contratada).

1.4.2 Módulo: Supervisão

Este serviço possibilita a monitoração constante da capacidade e da disponibilidade da infraestrutura de segurança do cliente. Este tipo de monitoração é ponto chave para os processos de gestão de capacidade e disponibilidade do ambiente, permitindo aos administradores:

- Compreender as atuais demandas sobre os recursos de segurança e criar previsões para futuras solicitações;
- Produzir um plano de capacidade que permitirá oferecer serviços na qualidade definida nos acordos de nível de serviço da organização;
- Avaliar se o nível de disponibilidade é sustentável e se possui um custo efetivo, permitindo o negócio atingir seus objetivos de forma consistente.

1.4.2.1 Como funciona?

A arquitetura de monitoração do SOC utiliza o protocolo SNMP para realizar os *healthchecks* nos componentes da infraestrutura do cliente.

Estas verificações são ativadas no momento de implantação do serviço, utilizando definições padrão de *thresholds*. Estes valores poderão ser ajustados com o apoio do cliente a fim de identificar quais situações normalmente não correspondem à normalidade dos serviços.

Se for identificado que algum componente atingiu certo nível de utilização (*threshold*), um alerta será gerado e será encaminhado para os técnicos responsáveis pela administração do ativo em questão.

As seguintes atividades serão executadas através do serviço de Supervisão:

- Acompanhamento da saúde dos dispositivos supervisionados 24x7;
- Comunicação de anomalias ao cliente, quando um componente monitorado apresentar índices não usuais.

O serviço não inclui o desenvolvimento ou a implantação de agentes personalizados de monitoração, oferecendo a monitorização da saúde dos dispositivos através de um número predefinido de itens, conforme lista abaixo. Entretanto, estes itens nem sempre são suportados por todas as tecnologias do mercado.

- Utilização da CPU;
- Utilização de memória;
- Utilização do disco;
- Estado das interfaces de rede;
- Temperatura;
- Número de sessões de VPN;
- Número de pacotes perdidos;
- Número de pacotes negado;
- Número de conexões;
- Estado do cluster;
- Estado de serviços.

1.4.2.2 Relatórios Mensais

Serão apresentados mensalmente ao cliente um conjunto de relatórios com as seguintes informações:

- Número de solicitações, incidentes e consultas efetuadas;
- Tempo médio de resolução das solicitações, incidentes e consultas efetuadas;
- Cumprimento de SLA;
- Número de notificações enviadas ao cliente devido a alertas detectados;

- Disponibilidade dos ativos monitorados;
- Número de alertas detectados nos ativos monitorados;
- Tempo sem serviço devido à manutenção programada nos ativos.

1.4.2.3 Requisitos Técnicos

Para que este serviço seja disponibilizado para o cliente, é necessário que os ativos que serão monitorados suportem os protocolos SNMPv3 (preferencialmente) ou SNMPv2c. Também é necessário que tais ativos sejam configurados para permitirem o acesso SNMP de leitura a partir da arquitetura de monitoração do SOC.

- *Sonda dedicada*: trata-se de uma sonda que será instalada no site do cliente para a coleta dos dados dos dispositivos monitorados. Utiliza-se a sonda dedicada em projetos em que o número de dispositivos gerenciados é grande o suficiente ou em casos em que os equipamentos monitorados estão em um local de rede que não é acessível facilmente por uma VPN ou conexão dedicada.

1.4.2.4 Requisitos Comerciais

O serviço de Supervisão requer a contratação do módulo de administração.

1.4.2.5 Requisitos de Conectividade

Este serviço necessita conectividade 24x7 entre o SOC e os equipamentos do cliente.

1.4.2.6 Atendimento

Na tabela abaixo é possível acompanhar a janela de atendimento para o serviço de Supervisão para cada tipo de atividade.

Serviço	Atendimento a		
	Incidentes	Solicitações	Consultas
Supervisão	24x7	12x7	12x7

Supervisão – Atendimento e Suporte

1.4.2.6.1.1 Incidentes

Os seguintes tipos de incidentes podem ocorrer para este serviço:

- Incidente num equipamento: indisponibilidade ou degradação da sonda de monitoração utilizada para o serviço;
- Notificação de alertas ao cliente que foram gerados pela ferramenta de monitoração.

1.4.2.6.1.2 Consultas

São previstas as seguintes consultas para este serviço:

- Lista de equipamentos supervisionados;
- Variáveis e limites de supervisão aplicados;
- Mapa de rede e de serviços;
- Lista de contatos autorizados pelo cliente.

1.4.2.6.1.3 Solicitações

São previstas as seguintes solicitações para este serviço:

- Modificação nos parâmetros de supervisão de um equipamento;
- Modificação massiva dos parâmetros de supervisão em uma lista de equipamentos;
- Modificação na lista de contatos autorizados do cliente;
- Modificação no mapa de rede ou no mapa de serviços do cliente.

1.4.3 Módulo: Administração

O módulo de serviço de Administração tem como objetivo disponibilizar um time de especialistas em segurança da informação para realizar customizações nas configurações dos equipamentos monitorados.

Veja as atividades previstas abaixo:

- **Atendimento & Suporte 24x7x365:** contempla a realização das tarefas operacionais solicitadas pelo cliente, tais como executar backup de configurações, gerenciamento de usuários, entre outros;
- **Resolução de incidentes de segurança:** os operadores de segurança passam a resolver incidentes de segurança que ocorrem nos dispositivos administrados, detectados pelo monitoramento ou informados pelos clientes;
- **Correção de vulnerabilidades:** ao identificar uma vulnerabilidade, o SOC torna-se responsável por executar a correção da mesma, tomando as devidas ações sobre itens gerenciados;
- **Análise de risco:** o SOC informará o cliente dos possíveis riscos de segurança identificados através da administração da infraestrutura ou através das ferramentas de administração;
- **Planejamento e implementação de mudanças**: contempla a avaliação e implementação de mudanças nos dispositivos por meio de solicitações do cliente ou por recomendação do SOC, baseados nas melhores práticas de gestão. Esta atividade não contempla mudanças na arquitetura ou funcionalidade dos elementos gerenciados;

- **<u>Gestão de suporte do fabricante:</u>** o SOC será responsável por acionar o suporte do fabricante (considerando que o ativo tenha tal suporte) em casos em que tal apoio seja necessário;
- **<u>Garantir o correto funcionamento dos dispositivos administrados:</u>** o SOC irá monitorar funcionamento dos dispositivos de forma proativa, visando garantir o bom funcionamento e a disponibilidade dos serviços;
- **<u>Manter e atualizar o software do dispositivo:</u>** o SOC irá atualizar o software sempre que recomendado pelo fabricante ou quando solicitado pelo cliente. Toda atualização será feita somente se autorizada pelo cliente, através do processo de gestão da mudança. Esta atividade inclui aplicação de patches para a resolução de incidentes, correção de vulnerabilidades e prevenção de incidentes de segurança;

1.4.3.1 Atendimento

Na tabela abaixo é possível acompanhar a janela de atendimento para o serviço de Administração para cada tipo de atividade.

Serviço	Atendimento a		
	Incidentes	Solicitações	Consultas
Administração – Janela de atendimento	24x7	12x5	12x5

Administração – Atendimento e suporte

1.4.3.1.1 Incidentes

Os seguintes tipos de incidentes podem ocorrer para este serviço:

- Incidente num equipamento: indisponibilidade ou degradação do serviço de um equipamento administrado.

1.4.3.1.2 Consultas

São previstas as seguintes consultas para este serviço:

- Lista de equipamentos administrados;
- Lista de alterações pré-autorizadas pelo cliente;
- Mapa de rede e de serviços;
- Lista de contatos autorizados pelo cliente;

1.4.3.1.3 Solicitações

São previstas as seguintes solicitações para este serviço:

- Alteração na política (regra em firewall, alerta IPS, etc.) de um equipamento;

- Modificação nos parâmetros de configuração de um equipamento;
- Modificação na lista de alterações pré-autorizadas pelo cliente;
- Modificação na lista de contatos autorizados do cliente;
- Modificação no mapa de rede ou no mapa de serviços do cliente.

1.4.3.2 Relatórios Mensais

Serão apresentados mensalmente ao cliente um relatório contendo as informações coletadas dos últimos 30 (trinta) dias.

Veja abaixo o conteúdo disponível nesse relatório:

1.4.3.2.1 Relatório de Tráfego

- Resumo Banda Utilizada;
- Resumo por sessão;
- Resumo por portas específicas (Configuradas previamente pelo SOC).

1.4.3.2.2 Relatório de Hardware

- Utilização da CPU;
- Utilização da Memória;

1.4.3.2.3 Relatório Filtro Web

- Resumo da Atividades Web;
- Resumo do Tempo de Navegação;
- Usuários Ativos por Período;
- Navegação Web por Acessos/Usuários;
- Sites Mais Visitados por Acesso/Usuário (Top 50);
- Usuários mais Ativos por Tempo de Navegação (Top 10);
- Usuários mais Ativos por Banda Utilizada (Top 20);
- Usuários Mais Bloqueados (Top 20);
- Principais Categorias da Web Visitadas;
- Principais Categoria e Sites por Banda Utilizada (Top 20);
- Principais Sites de Vídeo Streaming por Banda Utilizada;
- Categorias Mais Visitadas por Acesso (Top 20);
- Categorias Mais Visitadas por Tempo de Navegação (Top 10);
- Categorias Mais Bloqueadas (Top 20);
- Categorias Mais Visitadas por Banda Utilizada (Top 20);
- Sites Mais Visitados por Tempo de Navegação (Top 50);
- Sites Mais Visitados (e Categorias) por Banda Utilizada (Top 50);
- Sites Mais Bloqueados (Top 50).

1.4.3.2.4 Relatório de Usuários

- Principais usuários por banda utilizada;

1.4.3.2.5 Vítimas e Origens

- Principais Vítimas de Intrusões;
- Principais Vítimas de Intrusões (Crítica, Alta e Média);
- Principais Origens de Intrusões;

1.4.3.2.6 Relatório de Controle de Aplicações

- Distribuição de Aplicações de Alto Risco;
- Aplicações de Alto Risco (Classificação de 4 ou 5) identificados;
- Aplicações de Médio Risco (Classificação 3) identificados;

1.4.3.2.7 Controle de Aplicação por usuários

- Principais Usuários Permitidos pelo Controle de Aplicações;
- Principais Usuários Bloqueados pelo Controle de Aplicações;
- Principais Aplicações Liberadas por Banda Utilizada (Top 20)
- Principais Aplicações Bloqueadas por Sessões (Top 10);
- Principais Categorias de Aplicações por Banda Utilizada (Top 10);
- Divisão por Categorias de Todas as Aplicações, ordenadas por Banda Utilizada;
- Lista de Aplicações por Banda Utilizada (TOP 40);
- Lista de Aplicações por Sessões (TOP 40);
- Principais Aplicações Web por Banda Utilizada (Top 30);

1.4.3.2.8 Relatório de Prevenção de Incidentes

- Principais Intrusões por Severidade (Crítica, Alta e Média);
- Cronograma de Intrusões (Crítica, Alta e Média);
- Principais Intrusões por Tipo;
- Principais Intrusões Bloqueadas;
- Ataques sobre HTTP/HTTPs;

1.4.3.2.9 Relatório VPN e SSL VPN e IP Sec VPN

- Uso de Tráfego VPN;
- Login de usuário VPN;
- Logins autenticados;
- Falhas na Tentativa de Login;
- Principais Usuários VPN Dial-up;
- Principais Origens de VPN SSL por Banda Utilizada;
- Principais Usuários de VPN SSL por Banda Utilizada;
- Principais Usuários de VPN SSL por Duração do Acesso;
- Principais Túneis VPN Site-to-Site (IPsec) por Banda Utilizada

1.4.3.2.10 Relatório Redes Sociais

- Principais Usuários de Redes Sociais por Acessos;
- Principais Usuários de Redes Sociais por Tempo de Acesso;
- Principais Usuários de Redes Sociais por Banda Utilizada;

1.4.3.2.11 Malwares

- Principais Malwares Detectados;
- Principais Vitimas de Malwares;
- Principais Origens de Malwares;
- Cronograma dos Malwares.

1.4.3.2.12 Botnets

- Principais Botnets Detectados;
- Principais vítimas de Botnets;
- Principais Origens de Botnets;
- Cronograma dos Botnets;

1.4.3.2.13 Outros Itens

- Número total de dispositivos administrados;
- Número de incidentes, solicitações e consultas efetuadas;
- Número de incidentes, solicitações e consultas solucionadas;
- Tempo médio de resolução dos incidentes, solicitações e consultas efetuadas;
- Cumprimento de SLA;

1.4.3.3 Relatórios customizados

Não está contemplado a criação de relatórios que usem estrutura ou conteúdo dos detalhados acima. Caso seja necessário, deve ser detalhado nesse item em momento de construção da proposta.

1.4.3.4 Requisitos Gerais

Os seguintes devem ser observados para a prestação de serviço:

- A gestão de todos os usuários das ferramentas que compõem a solução de gestão será para uso exclusivo da **VIVO** ;
- O cliente não poderá gerenciar os dispositivos em que este serviço é prestado;
- A autenticação para acesso administrativo aos dispositivos ser dará através do serviço de autenticação da **VIVO** ;
- Os dispositivos gerenciados devem ser sincronizados com servidor de tempo (NTP) da **VIVO** .

1.4.3.5 Requisitos de Conectividade

Este serviço necessita conectividade 24x7x365 entre o SOC e os equipamentos. A solução técnica será definida no momento de ativação do serviço.

2 CONDIÇÕES DE PRESTAÇÃO DO SERVIÇO

2.1 ABERTURA DE CHAMADOS

As solicitações sobre o serviço deverão ser efetuadas a Central de Relacionamento da **VIVO** através do processo abaixo:

1. Entre em contato no número 0800 0151551;
2. Selecione a opção “OPÇÃO 3”;
3. Quando solicitado, digite o código 9016;
4. Pronto! Contato com o SOC estabelecido.

O atendimento é realizado 24 horas por dia, 7 dias por semana, 365 dias por ano de acordo com a jornada de atendimento contratada pelo cliente.

O cliente poderá designar até 03 (três) administradores de sua empresa, unidade de negócio ou filial para contato com a Central de Relacionamento, os nomes deverão ser informados durante o processo de implantação do serviço. A Central de Relacionamento da **VIVO** não efetua atendimento ao usuário final.

O SOC efetuará o acompanhamento das solicitações e das soluções dadas ao cliente. A cada solicitação será associado um número de registro da chamada e quando for o caso, um nível de severidade, conforme o grau crítico do problema avaliado.

2.2 FECHAMENTO DE CHAMADO

O chamado somente será concluído com o aceite dado por um dos três administradores designados pelo cliente, sendo o contato efetuado por telefone, e-mail ou via portal de atendimento on-line.

2.3 HORÁRIO DE ATENDIMENTO

Para os serviços na modalidade 8x5, o horário de atendimento é das 08:00 às 18:00 horas, de segunda a sexta.

Para os serviços na modalidade 12x5, o horário é das 08:00 às 20:00 horas, também de segunda a sexta.

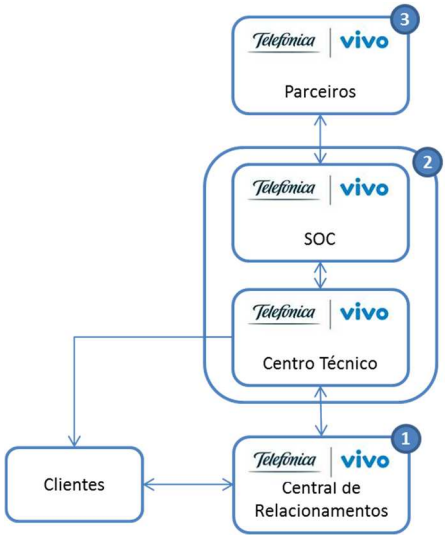
Para os serviços na modalidade 24x7, não há interrupção no horário de atendimento.

2.4 FLUXO DE ATENDIMENTO

Para controle das solicitações e da resolução das mesmas, bem como para o adequado acompanhamento do desempenho do serviço, o cliente deve instruir e garantir que não haverá interação direta de seus usuários finais com a Central de Relacionamento da **VIVO** , sendo tal atividade atribuída apenas à equipe de suporte do cliente.

No caso de necessidade de interação com o cliente para a resolução de algum problema na infraestrutura de segurança do cliente, a equipe técnica do SOC, através do Centro Técnico, entrará em contato com um dos três administradores designados pelo cliente, que serão os pontos focais.

O ponto de contato do cliente sempre será a Central de Relacionamento (nível 1), seja para abrir novas solicitações, reportar incidentes ou consultar o status de chamados abertos. A Central de Relacionamento é responsável por registrar todos os chamados dos clientes. Uma vez que se identificou que o caso está além das possibilidades de resolução pela própria Central, o chamado é direcionado para o Centro Técnico/SOC (nível 2) que, se necessário, aciona seus parceiros tecnológicos (nível 3) para atender o cliente.



Fluxo de Atendimento

2.5 NÍVEIS DE SUPORTE

O SOC disponibiliza três níveis de suporte para atendimento aos serviços contratados pelo cliente:

- **Suporte 1º Nível:** realizado pela equipe do SOC que trabalham 24x7 (vinte e quatro horas por dia, sete dias por semana) para atendimento a qualquer grau de severidade de incidentes ou solicitações;
- **Suporte 2º Nível:** realizado pela equipe do SOC que trabalha 8x5 (oito horas por dia, 5 dias por semana), podendo ser acionado fora deste horário pelo 1º Nível para cumprimento de SLO/SLA dos serviços;

- **Suporte 3º Nível:** realizado pela equipe de especialistas do SOC que trabalha 8x5 (oito horas por dia, 5 dias por semana), podendo ser acionada fora deste horário pelo 2º Nível para cumprimento de SLO/SLA dos serviços.

O relacionamento com os fornecedores ou parceiros envolvidos na solução dos problemas é de responsabilidade da equipe técnica do SOC **VIVO** .

2.5.1 Portal de Atendimento Online

O Portal de Atendimento Online exclusivo para os clientes VIVO com o objetivo melhorar a experiência na comunicação entre o time de especialistas de segurança do SOC e os responsáveis técnicos da (a) <NOME DO CLIENTE> através de um canal de comunicação totalmente digital.

O Sandas permite aos clientes acessar, acompanhar e gerenciar todas as consultas, solicitações e incidentes, independente do status. Veja abaixo algumas funcionalidades disponíveis:

- Visão Geral do status das solicitações e incidentes registrados no portal;
- Criação, alteração e acompanhamento de novos tickets através de portal web;
- Adição de comentários nos nas solicitações e incidentes abertos;
- Pesquisa por período de tempo, status, criticidade e tipo das solicitações e Incidentes;
- Consulta aos relatórios mensais emitidos pelo SOC em diretório on-line;

Os acessos ao portal poderão ser criados para até 5 (cinco) usuários cadastrados na lista de contatos autorizados do SOC. Não é permitido a liberação para empresas terceiras ou contatos que não constam na lista de contatos autorizados do SOC.

3 DETALHAMENTO ACORDO DE NÍVEL DE SERVIÇO

Este item tem como objetivo estabelecer e fornecer informações a respeito do acordo de nível de serviço que irá definir os padrões de qualidade da família de serviços MSS oferecidos pela **VIVO** .

3.1 DESCRIÇÃO DAS SEVERIDADES

As severidades são definidas de acordo com impacto do evento, conforme tabelas abaixo.

Incidentes de Serviço	Definição
Crítico	Evento que indisponibiliza os serviços de um ativo classificado como crítico
Alto	Evento que degrada os serviços de um ativo classificado como crítico ou que indisponibiliza os serviços de um ativo não crítico
Médio	Evento que degrada os serviços de um ativo classificado como não crítico
Baixo	Evento que não afeta os serviços

Critérios de Severidade – Incidentes

3.2 SLO DE PRESTAÇÃO DOS SERVIÇOS

Os serviços MSS são prestados pelo SOC considerando os seguintes objetivos de atendimento.

3.2.1.1 SLO de Incidentes

Serviços	Definição	Crítico	Alto	Médio	Baixo
Supervisão e Administração	**Tempo de atendimento** a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC.	15 min.	30 min.	1h.	2h.
Supervisão e Administração	**Tempo de resposta** a partir da comunicação do cliente até o primeiro diagnóstico do SOC.	1h.	1,5h.	3h.	6h.
Supervisão e Administração	**Tempo de resolução** a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	4h.	6h.	12h.	24h.
Supervisão e Administração	**Tempo de notificação** deste a detecção a partir da plataforma até comunicação do evento para o cliente.	15 min.	30 min.	1h.	1h.

Tabela 1 - SLO de Incidentes

3.2.1.2 SLO de Apresentação de Relatórios

Serviço	Definição	Prazo
Supervisão e Administração	**Tempo de entrega** de relatórios mensais	Até 5º dia útil do mês
Administração	**Tempo de entrega** de relatório após resolução de incidentes críticos	48 horas

Tabela 2 - SLO de Apresentação de Relatórios

3.2.1.3 SLO de Solicitações e Consultas

Serviço	Definição	Alto	Médio	Baixo
Supervisão e Administração	**Tempo de atendimento** de consultas a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	1h.	2h.	3h.
Supervisão e Administração	**Tempo de resolução** de consultas a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	8h.	10h.	16h.
Supervisão e Administração	**Tempo de atendimento** de solicitações a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	1h.	2h.	2h.
Supervisão e Administração	**Tempo de resolução** de solicitações a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	8h.	12h.	16h.

Tabela 3 - SLO de Solicitações e Consultas

3.2.2 SLA de Prestação dos Serviços

O SLA para os serviços de MSS segue as definições das tabelas abaixo.

Métrica	SLA	Aplica-se a
Tempo de Atendimento	95%	Consultas, requisições e incidentes.
Tempo de Resposta	95%	Consultas, requisições e incidentes.

Tempo de Notificação	95%	Consultas, requisições e incidentes.
Tempo de Resolução	95%	Consultas e requisições.

Tabela 4 - SLA

Somente se considera para efeitos de penalização:

- Incidentes Críticos e Altos;
- As requisições categorizadas como altas pelo cliente na abertura do chamado.

Assim, os itens que excedam e não cumpram o SLA definido estarão sujeitos a um desconto, que serão liquidadas mensalmente pela fórmula:

$$\mathrm{Vpd} = \frac{(\mathrm{Te} \times 100)}{(1.440 \times \mathrm{Nd})}$$

Na qual:

- Vpd = percentual de minutos excedidos no respectivo mês;
- Te = tempo excedido em minutos além do determinado na tabela de SLO para o serviço em questão;
- Nd = Número de dias no mês

Sendo constatado o não cumprimento do SLA, os índices de descontos, da tabela, abaixo, serão aplicados sobre o valor mensal a ser pago pelo cliente. Os descontos serão aplicados no mês subsequente ao mês da confirmação da ocorrência.

Percentual	Descontos %
0 < Vpd ≤ 2	0,5
2 < Vpd ≤ 4	1,0
4 < Vpd ≤ 6	2,5
6 < Vpd ≤ 10	5,0
10 < Vpd ≤ 20	7,5
Vpd > 20	10,0

Índices de descontos

3.2.2.1 Interrupções

A disponibilidade que garante o serviço obedece às seguintes condições:

- Não se contabilizarão dentro do tempo da não disponibilidade as interrupções do serviço que foram provocadas por causas imputáveis ao Cliente;
- O Cliente é responsável por facilitar o acesso a suas dependências, das pessoas designadas pela **VIVO** , para a resolução dos problemas, ou a operação do serviço que seja necessária. O tempo necessário para obter esta permissão está fora do cálculo da disponibilidade;
- A **VIVO** se reserva no direito de efetuar, mediante aviso prévio ao cliente, paradas técnicas que não se contabilizam no cômputo da disponibilidade;
- São excluídas interrupções do serviço devidas a causas de força maior (por exemplo, desastres naturais).

3.2.2.2 Períodos de manutenção

Por necessidade de manutenção, pode ser necessário interromper o serviço prestado ao cliente, com o objetivo de executar reconfigurações, atividades de manutenção, etc., na plataforma de prestação de serviços. Tais atividades serão executadas, necessariamente, durante um período pré-programado de manutenção.

3.2.2.3 Interrupções programadas

As interrupções programadas de disponibilidade do serviço, sejam elas pelas causas motivadas pelo item anterior, de períodos de manutenção, ou motivadas por alguma solicitação do Cliente, não serão contabilizadas para o cálculo da disponibilidade do serviço,

4 GESTÃO OPERACIONAL DO CONTRATO

A prestação dos serviços pela **VIVO** e o cumprimento do contrato a ser firmado deverão ser fiscalizados, monitorados e geridos pelas partes para fins de contínua avaliação e melhoria dos serviços prestados.

A gestão operacional do futuro contrato será feita através da gerência técnico-operacional da **VIVO** , que deverá zelar pelo bom desenvolvimento de todos os projetos e processos ligados aos serviços prestados ao Cliente, mantendo um canal de alto nível para comunicação entre as empresas.

5 PRESTADORAS DE SERVIÇOS CONTRATADAS PELA VIVO

A **VIVO** poderá contratar terceiros para a prestação dos serviços, sendo que, neste caso, ela será a única e diretamente responsável perante o Cliente por todos os serviços prestados por terceiros.

6 MATRIZ DE RESPONSABILIDADES

A seguinte matriz de responsabilidades governará o relacionamento operacional entre **Vivo** e o cliente.

Legenda:

Sigla	Significado
S	Solicitante
E	Executor
I	Informado
C	Consultado

Atividade	Responsabilidade	
	Vivo	Contratante

Supervisão		
Supervisão de possíveis links IP Internet conectados aos equipamentos de segurança gerenciados	**I**	**E**
Monitoração de disponibilidade dos equipamentos gerenciados	**E**	**I**
Monitoração de desempenho dos equipamentos gerenciados	**E**	**I**
Definição dos processos críticos a serem monitorados	**E**	ISC
Aprovar processos críticos a serem monitorados		**EI**
Monitoração (UP/DOWN) de processos específicos	**E**	**I**
Acionamento da contratante em caso de problema em processo monitorado	**E**	**I**
Configurar e suportar as ferramentas de supervisão	**E**	
Monitoração da capacidade atual dos equipamentos	**E**	**I**
Planejamento da capacidade e utilização dos equipamentos	**IC**	**E**
Geração de relatórios mensais de supervisão com indicação dos recursos gerenciados	**E**	**I**
Gestão de Acessos		
Criação/remoção de usuários, perfis de acesso e reset de senha para acesso a console administrativa	**E**	**SI**
Configuração do ativo gerenciado para suportar a integração com base de dados externa	**E**	**SI**
Integração das soluções de segurança com soluções de autenticação da contratante	**I**	**E**
Gestão de Incidentes e Problemas		
Identificar incidentes de segurança nos ativos gerenciados (exceto clientes com o módulo de notificação de incidentes)	**IC**	**E**
Responder a incidentes de hardware e software identificados nos ativos gerenciados	**E**	**IC**
Elaboração de relatórios de resposta aos incidentes de hardware e software identificados nos ativos gerenciados	**C**	**E**
Apoio na análise e resolução de incidentes e problemas nos ativos gerenciados	**E**	**I**
Manutenção do hardware dos equipamentos	**E**	**I**
Abertura de chamados nos fabricantes em caso de incidentes de hardware ou software	**E**	**I**
Monitoração de Eventos/Logs - Notificação de Incidentes		
Coletar e monitorar eventos/logs de segurança nos ativos gerenciados	**E**	**I**
Notificar contratante sobre alertas de segurança identificados pela monitoração de eventos/logs	**E**	**I**
Responder a incidentes de segurança identificados nos ativos gerenciados	**E**	**I**
Elaboração de relatórios de resposta aos incidentes de segurança identificados nos ativos gerenciados	**C**	**E**
Gestão de Mudanças		
Planejamento técnico de mudanças de configuração nos ativos gerenciados	**E**	**IC**
Planejamento técnica de mudanças de firmware nos ativos gerenciados	**E**	**IC**
Encaminhamento de solicitações de mudanças ao comitê aprovador de mudanças da contratante	**I**	**E**
Defesa da mudança de configuração pertinente ao ativo gerenciado dentro do comitê aprovador de mudanças	**E**	**E**
Defesa da mudança de firmware pertinente ao ativo gerenciado dentro do comitê aprovador de mudanças	**E**	**E**
Validação e aprovação de todas as mudanças que provoquem impactos nos serviços e negócios em produção	**I**	**E**

Implementação das mudanças de configurações nos ativos gerenciados	**E**	I
Implementação das mudanças de firmware nos ativos gerenciados	**E**	I
Administração – Atividades operacionais		
Gestão das configurações já ativas na implantação do projeto (ex: regras, políticas, componentes, etc.)	**E**	**ISC**
Ativação de novas funcionalidades equipamento de segurança não habilitados no momento da instalação	**IC**	**E**
Alterações na topologia que envolva a rede interna	**IC**	**E**
Consultorias técnicas que promovam melhorias de segurança na configuração dos ativos gerenciados.	**I**	**E**
Criação / remoção / alteração de regras e definição de parâmetros de bloqueio	**E**	**ISC**
Alteração dos parâmetros de mitigação em tempo real em casos de ataques	**E**	**ISC**
Correção de vulnerabilidades e riscos no equipamento gerenciado	**E**	**IC**
Análise de vulnerabilidades e regras (exceto para os clientes que contrataram esse serviço com a Telefônica | VIVO)	**IC**	**E**
Preparação dos procedimentos para backup e restore	**E**	**I**
Execução de rotinas programadas de backup e restore de dados	**E**	**I**
Esclarecimentos de dúvidas	**E**	**IS**
Suporte à sistemas operacionais, banco de dados, servidores de aplicação e estrutura de rede do ambiente da contratante	**I**	**E**
Gestão Administrativa		
Definição do processo de comunicação entre a contratante e a Telefônica | Vivo	**E**	**ISC**
Fornecer licenças e upgrades de ativos de propriedade da Telefônica | Vivo	**E**	**IS**
Gestão da versão de firmware	**E**	**I**
Manutenção / RMA		
Diagnóstico para identificação da necessidade de substituição do equipamento	**E**	**IS**
Solicitar o RMA do equipamento em caso de defeito	**E**	**IS**
Substituição do equipamento defeituoso em caso contemplado esse item no contrato	**E**	**IS**
Substituição do equipamento defeituoso em caso que não contemple esse item no contrato	**IC**	**E**
Liberação de acesso e acompanhamento do profissional nas dependências do cliente	**I**	**EC**

7 RESPONSABILIDADE DO CLIENTE

Clientes que venham a contratar serviços da **VIVO** estarão assumindo as seguintes responsabilidades:

- Fornecer no prazo de até 15 (quinze) dias após o fechamento do contrato um período de comum acordo com o PMO da Vivo para a instalação dos equipamentos considerado nessa proposta;
- Fornecer todas as informações necessárias para o dimensionamento e embasamento técnico dessa proposta técnica e comercial;

- Informar a **VIVO** sobre qualquer mudança com relação à prestação dos serviços, com a devida antecedência, permitindo que a mesma tenha tempo suficiente para preparar e implementar as alterações necessárias, conforme tais alterações ou mudanças afetem a prestação dos serviços. O Cliente deverá fornecer informações suficientes com relação às suas necessidades;
- Informar a **VIVO** com antecedência mínima de 30 (trinta) dias sobre qualquer mudança que possa afetar a prestação de Serviços
- Zelar pela conservação e correto manuseio da infraestrutura e equipamentos disponibilizados pela **VIVO** , responsabilizando-se pelos eventuais danos, pessoais e materiais, decorrentes de ações e utilizações indevidas por parte de seu pessoal ou de seus equipamentos;
- Informar internamente e aos seus outros prestadores de serviços, o escopo de contrato com a **VIVO**, quando relacionado a suas atividades;
- Não gerenciar diretamente nenhum funcionário ou terceiros da **VIVO** alocados ou em atendimento nos sites do cliente;
- Em caso de cancelamento do serviço por qualquer de ambas as partes, o cliente se compromete em desinstalar os equipamentos e emitir a documentação necessária a retirada do equipamento.

7.1 PRÉ-REQUISITOS PARA A INSTALAÇÃO, ATIVAÇÃO E ADMINISTRAÇÃO DO SERVIÇO

Para que o time de especialistas da VIVO seja capaz de instalar, ativar e administrar o serviço contratado pelo cliente, é necessário que alguns pré-requisitos de infraestrutura física, lógica e recursos humanos sejam disponibilizados. Veja abaixo a lista completa.

- Fornecer link de Internet 100% instalado e funcionando corretamente;
- Disponibilizar local específico com climatização e condições adequadas para o armazenamento físico do equipamento da VIVO na localidade do cliente;
- Fornecer cabeamento, adaptadores e conectores ou qualquer para outro item necessário para integrar o equipamento na rede interna do cliente;
- Disponibilizar topologia completa da rede interna atualizada;
- Fornecer política de segurança que será configurada no equipamento como: regras de firewall, categorias de filtros de conteúdo que serão bloqueadas, entre outros;
- Dedicar um profissional para acompanhar todo o processo de instalação e ativação do serviço.

8 RESPONSABILIDADE DA VIVO

A **VIVO** assume as seguintes responsabilidades perante ao cliente:

- Designar um profissional **VIVO** que será ponto focal com o cliente
- Executar os serviços de acordo com o escopo descrito nessa proposta e níveis de serviço;
- Executar todas as atividades dentro dos padrões de qualidade **VIVO** e conforme estabelecido no contrato com o cliente;
- Cumprir os prazos estabelecidos nas atividades do projeto, desde que as responsabilidades do cliente sejam atendidas previamente a criação do cronograma de ativação do serviço;
- Gerenciamento proativo do serviço incluindo o fornecimento da Central de Atendimento.